

Active Scanning: Vulnerability Scanning, Sub-technique T1595.002

- Enterprise

Archived: 2026-04-05 15:31:49 UTC

Adversaries may scan victims for vulnerabilities that can be used during targeting. Vulnerability scans typically check if the configuration of a target host/application (ex: software and version) potentially aligns with the target of a specific exploit the adversary may seek to use.

These scans may also include more broad attempts to [Gather Victim Host Information](#) that can be used to identify more commonly known, exploitable vulnerabilities. Vulnerability scans typically harvest running software and version numbers via server banners, listening ports, or other network artifacts.^[1] Information from these scans may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](#) or [Search Open Technical Databases](#)), establishing operational resources (ex: [Develop Capabilities](#) or [Obtain Capabilities](#)), and/or initial access (ex: [Exploit Public-Facing Application](#)).

Source: <https://attack.mitre.org/techniques/T1595/002>